

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	X	
	:	
UNITED STATES OF AMERICA	:	
	:	
- v. -	:	S1 23 Cr. 430 (KPF)
ROMAN STORM,	:	
	:	
Defendant.	:	
-----	X	

**THE GOVERNMENT’S OPPOSITION TO THE DEFENDANT’S MOTIONS TO
EXCLUDE TESTIMONY OF THE GOVERNMENT’S EXPERT WITNESSES**

JAY CLAYTON
United States Attorney
Southern District of New York

Ben Arad
Benjamin A. Gianforti
Thane Rehn
Assistant United States Attorneys

Kevin Mosley
Special Assistant United States Attorney
- Of Counsel -

TABLE OF CONTENTS

INTRODUCTION	1
ARGUMENT	2
I. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Philip Werlau2	
A. The Defendant’s Challenges to Werlau’s Qualifications Are Meritless.....	3
B. Werlau’s Testimony that the February 2022 Upgrade to the Tornado Cash Service Implemented a New Incentive for Relayers to Purchase Torn Tokens Is Admissible	6
C. Werlau’s Testimony that the February 2022 Upgrade to the Tornado Cash Service Created a Way to Monetize the Service Is Admissible.....	8
D. Werlau’s Testimony Regarding Changes that Could Have Been Implemented to the Tornado Cash Service Is Admissible.....	9
E. Werlau’s Testimony Regarding the “Gas Ratio” Is Admissible.....	14
II. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Stephan George	21
III. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Joel DeCapua.....	24
A. Expert Testimony Based in Part on Hearsay Is Admissible, and the “Officer Expert” Cases on Which the Defendant Relies Are Inapposite	25
B. DeCapua’s Proposed Testimony Does Not Convey Hearsay or Violate the Confrontation Clause	29
IV. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of John Pisa-Relli.....	31
CONCLUSION.....	33

TABLE OF AUTHORITIES

Cases

<i>Alto v. Sun Pharm. Indus.</i> , 2021 WL 4803582 (S.D.N.Y. Oct. 13, 2021)	4
<i>Bank of China, New York Branch v. NBM LLC</i> , 359 F.3d 171 (2d Cir. 2004)	33
<i>Broker Genius, Inc. v. Zalta</i> , 280 F.Supp.3d 495 (S.D.N.Y. 2017)	7
<i>Capri Sun GmbH v. Am. Beverage Corp.</i> , 595 F. Supp. 3d 83 (S.D.N.Y. 2022)	21
<i>Davis v. Sig Sauer, Inc.</i> , 126 F.4th 1213 (6th Cir. 2025)	12, 13
<i>DoubleLine Cap. LP v. Odebrecht Fin., Ltd.</i> , 2024 WL 1115944 (S.D.N.Y. Mar. 14, 2024)	21
<i>Gussack Realty Co. v. Xerox Corp.</i> , 224 F.3d 85 (2d Cir. 2000)	22
<i>Henkel v. Wagner</i> , 2016 WL 1271062 (S.D.N.Y. Mar. 29, 2016)	19
<i>In re 650 Fifth Ave. & Related Properties</i> , 2017 WL 6419014 (S.D.N.Y. May 30, 2017)	32
<i>In re LIBOR-Based Fin. Instruments Antitrust Litig.</i> , 299 F. Supp. 3d 430 (S.D.N.Y. 2018)	4
<i>In re Zyprexa Prod.</i> , 489 F. Supp. 2d 230 (E.D.N.Y. 2007)	4
<i>McCormick v. Cleaver Brooks Co.</i> , 561 Fed. Appx. 121 (2d Cir. 2014)	12
<i>Peerless Ins. Co. v. Marley Engineered Prods. LLC</i> , 2008 WL 7440158 (E.D.N.Y. June 12, 2008)	4
<i>Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC</i> , 691 F. Supp. 2d 448 (S.D.N.Y. 2010)	5
<i>PRCM Advisers LLC v. Two Harbors Inv. Corp.</i> , 2025 WL 1276513 (S.D.N.Y. May 2, 2025)	21, 22
<i>Restivo v. Hessemann</i> , 846 F.3d 547 (2d Cir. 2017)	20
<i>Salazar v. United States</i> , 2019 WL 948865 (S.D.N.Y. Feb. 11, 2019)	12

<i>SEC v. Terraform Labs Pte. Ltd.</i> , 708 F. Supp. 3d 450 (S.D.N.Y. 2023)	6, 7
<i>SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.</i> , 2019 WL 7816487 (S.D.N.Y. Dec. 11, 2019)	7-8
<i>United States v. Diakhoumpa</i> , 171 F. Supp. 3d 148 (S.D.N.Y. 2016)	28
<i>United States v. Dukajgini</i> , 326 F.3d 45 (2d Cir. 2003).....	26, 27
<i>United States v. Dupree</i> , 2012 WL 5333946 (E.D.N.Y. Oct. 26, 2012)	14, 15
<i>United States v. Ferguson</i> 676 F.3d 260 (2d Cir. 2011)	5
<i>United States v. Joseph</i> , 542 F.3d 13 (2d Cir. 2008)	5
<i>United States v. Locascio</i> , 6 F.3d 924 (2d Cir. 1993)	27
<i>United States v. Mejia</i> , 545 F.3d 179 (2d Cir. 2008)	26, 28-29
<i>United States v. Napout</i> , 963 F.3d 163 (2d Cir. 2020)	18, 19, 20
<i>United States v. Prevezon Holdings, Ltd.</i> , 251 F. Supp. 3d 684 (S.D.N.Y. 2017)	28
<i>United States v. Sterlingov</i> , 719 F. Supp. 3d 65 (D.D.C. 2024)	29
<i>United States v. Torres</i> , 2021 WL 1947503 (S.D.N.Y. May 13, 2021)	27-28
<i>United States v. Whitehead</i> , 579 F. App'x 46 (2d Cir. 2014)	13-14
<i>Washington v. Kellwood Co.</i> , 105 F. Supp. 3d 293 (S.D.N.Y. 2015)	3-4, 5

Statutes

Fed. R. Crim. P. 32.2	24, 25
Fed. R. Evid. 703	24, 21, 22, 27
Fed. R. Evid. 702	3, 18
Fed. R. Evid. 403	10, 11

INTRODUCTION

At trial, the Government plans to introduce testimony and analyses from three expert witnesses. First, the Government plans to call Philip Werlau, a software developer who specializes in blockchain and smart contract investigations, and who has analyzed the computer code underlying various features of the Tornado Cash service and will provide an overview of how these features worked during the time period charged in the Indictment, including various changes and upgrades that were made over time. This testimony is rooted in an analysis of computer code that a lay jury cannot be expected to otherwise understand. Such testimony is necessary and appropriate to aid the jury in understanding how the Tornado Cash service operated, one of the central disputed issues in the case, and courts routinely admit exactly this type of evidence in cases involving computer code. The Government's other two expert witnesses are Joel DeCapua, an FBI Special Agent, and Stephan George, an IRS-CI Special Agent, both of whom have extensive experience in tracing cryptocurrency transactions using blockchain data. DeCapua will testify about the flow of funds into the Tornado Cash service, including the flow of funds from certain criminal incidents. George will testify about the defendant's receipt of funds from his involvement with the Tornado Cash service. The testimony of both experts is the product of extensive financial tracing and analysis of blockchain data and more traditional financial records. This type of expert tracing testimony is routinely admitted in cases involving money laundering and other financial crimes, and is necessary and appropriate to aid the jury in considering the financial evidence in the case.

The defendant's motion to exclude the testimony of these three experts, which seeks total preclusion but is focused only on discrete aspects of their testimony, is based on a misreading of the expert disclosures and is inconsistent with the case law. Each of these experts should be allowed to testify in full.

ARGUMENT

I. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Philip Werlau

The Government intends to call Philip Werlau, a software developer who specializes in blockchain and smart contract investigations, to testify about how the Tornado Cash service operated based on his review of the computer code underlying various features of the service, as well as related materials such as informational and instructional documents authored by the Tornado Cash founders. (Dkt. 158-1 (“Werlau Disclosure”)). Based on Werlau’s review of the code, he will generally testify about how the Tornado Cash service had multiple features that together worked in combination to conceal the connection between customer deposits and withdrawals. (*Id.* ¶ 6). He will also provide granular computer code-based testimony that will explain, among other things: how the Tornado Cash website, the Tornado Cash Ethereum domain, and the Tornado Cash graphical user interface (the “UI”) were interconnected and were controlled by the Tornado Cash founders (*id.* ¶¶ 7-11); how the founders also created a non-graphical “command line interface” (the “CLI”) that the defendant controlled and oversaw updates to over time (*id.* ¶ 12); which features of the Tornado Cash service were changeable and unchangeable, and how certain features were upgraded over time, with a particular focus on a major upgrade to many of the features of the service that took place in February 2022 (*id.* ¶¶ 14-16); how the changes that were made in February 2022 illustrate the types of changes that the Tornado Cash founders could make and demonstrate that they could have made additional changes to only allow authorized users to use certain features of the service (*id.* ¶¶ 17-18); a change made to the UI in April 2022 after OFAC announced that a particular North Korea-linked Ethereum address was sanctioned, and how that change illustrates that the founders could have made other changes to the UI and other features of the Tornado Cash service at that time (*id.* ¶ 19); and how blockchain data

and the code can be used to identify the percentage of Tornado Cash withdrawals that used a relay, and the percentage of Tornado Cash deposits that used the UI or the CLI (*id.* ¶ 21-22).

The defendant's motion makes five primary arguments against the admissibility of Werlau's testimony or particular components of it. First, the defendant argues that Werlau lacks sufficient qualifications to testify about blockchain technology and "tokenomics." (Dkt. 158 at 8-11). Second, the defendant argues that Werlau should not be permitted to testify about how changes made to the Tornado Cash service served to "increase market demand" for TORN tokens. (*Id.* at 12-14). Third, the defendant argues that Werlau should not be permitted to testify regarding the "monetization" of the Tornado Cash service. (*Id.* at 14-15). Fourth, the defendant argues that Werlau should not be permitted to testify about the feasibility of implementing KYC features in the Tornado Cash service. (*Id.* at 15-19). And finally, the defendant argues that Werlau should be precluded from testifying about the usage of the UI and CLI based on the gas ratio analysis, based in part on the defendant's mistaken view that Werlau did not perform the analysis himself. All of the defendant's arguments are meritless and rest in large part on misreading the scope and nature of Werlau's testimony as set forth in the disclosure.

A. The Defendant's Challenges to Werlau's Qualifications Are Meritless

The defendant first argues that Werlau "lacks sufficient qualifications" to offer the disclosed expert opinions, focusing on Werlau's lack of a relevant degree or peer-reviewed research. Those arguments are meritless in multiple respects. First, to the extent that the defendant is suggesting that formal academic training or peer-reviewed publications are a prerequisite to expert testimony, those arguments are simply incorrect. Federal Rule of Evidence 702 provides that a witness may be "qualified as an expert by knowledge, skill, experience, training, or education," and "the court must examine the totality of the witness's background to determine whether he exhibits *any one or more* of the[se] qualifications." *Washington v. Kellwood Co.*, 105

F. Supp. 3d 293, 304 (S.D.N.Y. 2015) (emphasis added). The Second Circuit “has adopted a liberal standard for qualifying an expert and there is no requirement that a witness have formal education or training before being qualified as an expert.” *Peerless Ins. Co. v. Marley Engineered Prods. LLC*, No. 05 Civ. 4848 (AKT), 2008 WL 7440158, at *2 (E.D.N.Y. June 12, 2008). “[A] lack of formal training does not necessarily disqualify an expert from testifying if he or she has equivalent relevant practical experience.” *In re LIBOR-Based Fin. Instruments Antitrust Litig.*, 299 F. Supp. 3d 430, 466 (S.D.N.Y. 2018); *see also Alto v. Sun Pharm. Indus.*, 2021 WL 4803582, at *2 (S.D.N.Y. Oct. 13, 2021) (even where an expert “lacks formal training in a given area” he may still be qualified to testify based on “‘practical experience’ or ‘specialized knowledge’” (citation omitted)); *In re Zyprexa Prod.*, 489 F. Supp. 2d 230, 282 (E.D.N.Y. 2007) (attacks on an expert’s “educational or other experiential background” go to weight, not admissibility (citation omitted)).

Here, Mr. Werlau’s “practical experience” for more than a decade as a software developer makes him fully qualified to review computer code and explain how it functions. Of note, his software development experience includes development of software that is closely analogous to the features of the Tornado Cash service that he reviewed for this case, including his experience developing an Ethereum-based platform and associated web-based user interface, and multiple smart contracts that integrated with the user interface. And Werlau has conducted multiple smart contract code audits and developed a specialized platform for “Web3” (i.e., blockchain technology-based) incident response. (Werlau Disclosure at 1). The defendant suggests that this experience is not applicable to “DeFi protocols such as Tornado Cash” (Dkt. 158 at 8), but he offers no basis to suggest that term refers to a separate category of expertise than Werlau’s expertise in blockchain-related computer code. As the defendant’s own expert report explains, the term “DeFi protocol” as applied to Tornado Cash is just a term used to encompass the interlocking

features of Tornado Cash, which are analyzed through review of the “developer documentation and source code for the Tornado Cash smart contracts, and source code for the Tornado Cash UI and CLI.” (Dkt. 159-4 (“Edman Disclosure”) ¶ 23). Those are the same materials that Werlau examined, and his years of experience developing, reviewing, and auditing source code for smart contracts and for blockchain-related applications and user interfaces is exactly the sort of practical experience that qualifies him to provide expert testimony regarding those materials. *See, e.g., Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 691 F. Supp. 2d 448, 473 (S.D.N.Y. 2010) (noting that an expert’s testimony may be based on his “years of experience” in a particular industry, upon a showing that the witness’s “experience provides a reliable foundation for his or her testimony”).

To be sure, the defendant is free to cross-examine Werlau on both his qualifications and his analysis, but these issues do not provide a basis to preclude him from testifying. *See United States v. Joseph*, 542 F.3d 13, 21-22 (2d Cir. 2008) (emphasizing that “the place to quibble with [an expert’s] academic training is on cross-examination and goes to his testimony’s weight ... not its admissibility”) (citation and internal quotation marks omitted), *abrogated on other grounds by United States v. Ferguson*, 676 F.3d 260, 276 n.14 (2d Cir. 2011). The defendant relies on cases in which courts have precluded expert witnesses based on a mismatch between the expert’s field of expertise and the topics on which his testimony is being offered (Dkt. 158 at 10-11), but none of those cases applies here. Werlau is not like a “marketer” who is being offered to testify about “contract negotiations” (*id.*), but is a software developer with extensive experience developing, reviewing, and auditing the computer code for the very types of software programs at issue here.

The law simply requires that the witness’s expertise be in a “general field closely related to the subject matter in question.” *Washington*, 105 F.Supp.3d at 305. Here, Werlau’s specific

expertise in writing, reviewing, and analyzing computer code for blockchain-related applications and smart contracts is far more tailored to the subject matter of his testimony than the law requires. Indeed, in a recent decision involving the computer code expert that the defendant seeks to use in this case, Dr. Matthew Edman, a court in this District rejected exactly the sort of hairsplitting of computer code expertise topics that the defendant is now advocating. *SEC v. Terraform Labs Pte. Ltd.*, 708 F. Supp. 3d 450, 466 (S.D.N.Y. 2023) (rejecting argument that blockchain-related computer code expert also needed expertise in “financial payment systems,” where expert had formed his opinions “by examining the source code of a server and its programming,” and noting that “[t]here is no indication that the features of or methods for analyzing source code differ when a financial payment system is involved”).

Finally, the defendant’s suggestions that Werlau only gained relevant experience in connection with this litigation (Dkt. 158 at 11) are belied by the Werlau disclosure. Werlau has more than a decade of experience in software development, and has been specifically working with smart contracts and other relevant blockchain-related products since 2021, long before his involvement in this case.

B. Werlau’s Testimony that the February 2022 Upgrade to the Tornado Cash Service Implemented a New Incentive for Relayers to Purchase Torn Tokens Is Admissible

The defendant’s next argument against Werlau’s testimony appears to be limited to three words in Paragraph 16 of the Werlau disclosure regarding how the February 2022 upgrade “increased market demand” for TORN tokens. (Dkt. 158 at 12; *see* Werlau Disclosure ¶ 16). That argument is premised on a misreading of Werlau’s testimony, which is simply based on an explanation of the February 2022 upgrade and is not an exercise in economic analysis or valuation. Specifically, based on his review of the computer code, Werlau has determined that the February 2022 upgrade included a new smart contract—the Relayer Registry—that was used to assign

relayers to particular withdrawals from which they earned fees, and that “[t]o be included in the Relayer Registry, relayers had to obtain” TORN tokens. (Werlau Disclosure ¶¶ 15(b)(i); 16). The effect of this change was that it “required relayers to purchase TORN tokens, creating increased market demand for those tokens.” (*Id.* ¶ 16). Whereas relayers previously did not need to purchase TORN tokens to be assigned withdrawals, after the February 2022 upgrade, they both had to make an initial purchase of TORN tokens, and they “had an ongoing requirement to purchase more TORN tokens to maintain their position in the Relayer Registry.” (*Id.*). While the defendant tries to insinuate otherwise, Werlau is not offering any opinion on the price of TORN or the “actual market impact” of the functioning of the Relayer Registry. (Dkt. 158 at 13-14).

Contrary to the defendant’s assertions, this testimony does not require expertise in economics or “the valuation of cryptocurrency tokens.” (Dkt. 158 at 12). The Government agrees that Werlau is not an expert on those topics. Rather, his testimony simply explains how the code worked to create a need for would-be relayers to purchase TORN tokens that did not previously exist, by requiring the relayers to purchase these tokens to be included in the Relayer Registry. To understand that fact requires an expert who can explain how the computer code worked, but the Government is not seeking to introduce evidence about valuation or price impacts, and Werlau will not opine on those topics. Computer code experts routinely are called to testify about the functional effect of software design, which requires expertise in reviewing source code but not other unrelated fields such as economics. *See, e.g., Broker Genius, Inc. v. Zalta*, 280 F.Supp.3d 495, 501 (S.D.N.Y. 2017) (discussing testimony of computer code expert that software program was “able to prioritize urgent price changes and thereby accommodate an increased number of users”); *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, No. 18 Civ. 5427 (JSR), 2019 WL 7816487, at *1 (S.D.N.Y. Dec. 11, 2019) (relying on “expert report affirming the

mechanics of this [software] redesign and supporting it with an explanation of the source code”).¹ Accordingly, the defendant’s arguments for precluding Werlau’s testimony on this topic should be rejected.

C. Werlau’s Testimony that the February 2022 Upgrade to the Tornado Cash Service Created a Way to Monetize the Service Is Admissible

The defendant’s next argument is a variation on his “market demand” argument. He contends that Werlau should not be permitted to testify that the February 2022 upgrade created a new way for the Tornado Cash service to “monetize its technology.” As with the defendant’s “market demand” argument, his “monetization” argument is premised on a misrepresentation of Werlau’s disclosure. Werlau’s testimony is rooted in a detailed description of how the different components of the Tornado Cash service worked together to generate a stream of payments of TORN tokens to TORN token holders who held their tokens in the Governance smart contract. In particular, the defendant and his co-conspirators created a new smart contract called the “Fee Manager, which would determine a commission in TORN tokens to be paid by the relayer” each time the relayer was selected to conduct a withdrawal. (Werlau Disclosure ¶ 15(b)(iv)).

The defendant does not challenge anything about Werlau’s analysis of the source code for these smart contracts or his description of how they functioned. Instead, he argues that Werlau should not be able to describe these payments from relayers as a “monetization” of the technology.

¹ The defendant does not challenge any of the actual opinions about or descriptions of the software upgrade set forth in paragraphs 15 and 16 of the Werlau disclosure, but focuses instead on the use of the term “increased market demand.” Those arguments are meritless because “market demand” is not a technical term but a commonly used term being used in its ordinary sense. *See, e.g.,* Michael Paulson, *The Price of a Show*, N.Y. Times, Mar. 23, 2025, <https://www.nytimes.com/2025/03/23/briefing/broadway-ticket-prices.html> (“Some people don’t like it when I say this, but ticket prices are set to reflect market demand.”). But even if the defendant’s arguments had any merit, the only result would be to preclude the use of the term “market demand” while still allowing Werlau to explain that the February 2022 upgrade created a new requirement for relayers to purchase TORN tokens to be included in the Relayer Registry.

But the only basis for that argument is the assertion, offered without citation, that “monetization of blockchain technology is an extremely complex topic.” (Dkt. 158 at 15). Werlau’s testimony will not be a general treatise on monetization, but instead a functional description of how the software worked; namely, that it generated payments that TORN token holders could receive. Werlau is not offering some technical definition of “monetization” that requires “monetization expertise” (whatever that would be). Rather, he is using the term in its ordinary commonplace meaning: to make money from something. *See, e.g.,* Jessica Testa, *Amazon Gets into the LeBron James Business*, N.Y. Times, Mar. 26, 2025, <https://www.nytimes.com/2025/03/26/business/media/lebron-james-podcast-amazon-wonderly.html> (“Sports is a category that monetizes really, really well.”). Based on Werlau’s analysis of the source code, he has determined that it created a stream of payments, and “monetization” is a fair and accurate description of that expert conclusion that will be comprehensible to the jury.

Because Werlau’s testimony is properly rooted in his expert analysis of how the software underlying various features of the Tornado Cash service worked, and because he uses ordinary language to describe the functional effect of the software, his testimony should not be precluded.²

D. Werlau’s Testimony Regarding Changes that Could Have Been Implemented to the Tornado Cash Service Is Admissible

The defendant next argues that Werlau should not be permitted to testify about additional changes to the Tornado Cash service that the defendant and his co-founders could have

² The defendant also repeats in this section his arguments that the Government’s witnesses should not be permitted to refer to the Tornado Cash service as a “service.” As discussed in the Government’s response to the defendant’s motion *in limine* on that topic, those arguments fail for a similar reason. (Dkt. 173 at 37-40). “Service” is not a technical or legal term but an ordinary description of the way the Tornado Cash features worked together as alleged in the Indictment. The defendant may challenge the factual basis for that description—that is what a trial is for. But he offers no authority for his attempt to prevent the Government from describing the facts using ordinary non-legal terminology.

implemented upon learning about money laundering and sanctions violations. (Dkt. 158 at 15-18). The defendant makes two arguments here. First, he contends that Werlau’s experience and analysis are insufficient to support his conclusions. Second, he argues that the testimony is not relevant or inadmissible under Rule 403. Neither argument holds water.

The defendant’s first argument, as with so many of his other arguments, simply ignores substantial parts of Werlau’s disclosure. The defendant asserts that Werlau lacks qualifications in “the area of KYC or anti-money laundering.” (Dkt. 158 at 16). But that misconstrues Werlau’s testimony. To start, as his disclosure states, Werlau has led “multiple investigations into cryptocurrency transactions related to hacking and money laundering, conducting smart contract code audits for government institutions and large blockchain companies,” and he has led a team that built a specialized application to be used in Web3 incident response. (Werlau Disclosure at 1). On top of that, Werlau has developed a customer-facing web interface for a blockchain project and multiple smart contracts and back-end infrastructure that interacted with and supported this platform. (*Id.*). This experience is exactly what enables Werlau to analyze the UI, smart contracts, and other features of the Tornado Cash service to determine how the code worked and whether it could have been changed in response to criminal exploits—this is what he has been doing professionally for years. This in turn, supplies ample basis to call for Werlau simply to testify that there was nothing from a *code* standpoint that prevented the defendant and his co-conspirators from implementing changes to features of the Tornado Cash service they controlled to allow them to identify users and block transactions from using those features. Contrary to the defendant’s statement, the Government is not calling Werlau as an expert on KYC or anti-money laundering (“AML”) controls.

Next, the defendant asserts that Werlau “does not explain how he came to his conclusion.” (Dkt. 158 at 16). But the disclosure sets forth the basis for the conclusion in detail. Werlau explains at length a number of changes that the defendant and his co-conspirators made to the Tornado Cash service in February 2022, including changes that implemented certain new “Registry” smart contracts to be used as part of the deposit and withdrawal process. (Werlau Disclosure ¶¶ 14-17). Werlau then explains how these changes to the code are themselves a model that could be used to implement a “registry of authorized users” that would allow the service to confirm the identity of people making deposits and withdrawals. (*Id.* ¶ 18). The defendant does not mount any critique of this analysis; instead, he just asserts that Werlau does not explain how this user registry “would exist in the context of a DeFi application in which users maintain control over their assets.” (Dkt. 158 at 17). But that argument is both unsupported and illogical, as there is nothing beyond the defense’s say-so about why a service could not have a user registry and also allow its users to control their own assets. The defense may attempt to introduce evidence to that effect at trial (although they have not disclosed any such evidence or expert testimony supporting that position), but defense counsel’s views are not a basis to preclude probative expert testimony.

In fact, Werlau’s disclosure explains exactly how multiple other smart contracts worked together to effectuate deposits and withdrawals, and then explains that an additional smart contract could have been integrated into the architecture in the same way. (Werlau Disclosure ¶ 18 (explaining that the Router smart contract was programmed to “call both the Instance Registry and Relayer Registry as part of each relayed withdrawal,” and that the founders “could also have implemented a new smart contract with a registry of authorized users, and could have programmed the Router to call that smart contract”)). Werlau draws a similar conclusion about changes that could have been made to implement sanctions screening, also by analogy to the February and April

2022 changes that were actually made. (Werlau Disclosure ¶ 19). The defendant is free to attack these conclusions on cross-examination or during his own case, but his attempt to suggest that Werlau’s expert analysis of the source code is not adequately explained is groundless. Similarly, the defense argument that Werlau has not identified any other “DeFi protocols” that have implemented a KYC function is not relevant to whether the Tornado Cash service, based on the code underlying its component features, could have done so.

Nor is the defendant helped by characterizing this testimony as engaging in “hypotheticals.” It is well established that expert testimony addressing hypothetical questions is admissible. *See McCormick v. Cleaver Brooks Co.*, 561 Fed. Appx. 121, 123 (2d Cir. 2014); *Salazar v. United States*, 2019 WL 948865, at *3 (S.D.N.Y. Feb. 11, 2019). Relatedly, it is well established that experts are permitted to offer relevant opinions about available alternatives. *E.g.*, *Davis v. Sig Sauer, Inc.*, 126 F.4th 1213, 1227 (6th Cir. 2025) (district court erred in excluding expert testimony regarding existence of “reasonable alternative designs” for firearm).

The defendant’s next argument is that testimony about what measures the Tornado Cash founders could have implemented in response to money laundering and sanctions violations is “not relevant.” (Dkt. 158 at 17-18). That argument is nothing short of astonishing in light of the positions the defendant has staked out in this case. As far as the Government can make out from the defendant’s filings, he does not seriously contest that the Tornado Cash service was used for large-scale money laundering and sanctions violations, nor that he knew about this. Instead, his defense appears to be that, as he said in the first sentence of his motion to dismiss the Indictment, Tornado Cash “quickly became fully decentralized (i.e., not in his, his company’s or anyone else’s control.” (Dkt. 37-1 at 1; *see also, e.g., id.* (“the Tornado Cash protocol was developed and became immutable before the alleged criminal conduct that is at the center of the money laundering count

even occurred”); *id.* at 2 (“by the time of the alleged sanctionable conduct, the Tornado Cash protocol was immutable and publicly available, and there was nothing Mr. Storm or anyone else could do to prevent a sanctioned entity from using it”).

In short, one issue that appears certain to be hotly contested at trial is the degree to which the defendant and his co-conspirators could exercise control over and make changes to various features of the Tornado Cash service during the period of the charged conspiracies. Indeed, in response to one of the defendant’s many motions raising this very issue, the Court has recognized that “at trial, the Government will bear the burden to prove that Defendant conspired with others to violate IEEPA by means of the features [of the Tornado Cash service] over which they had control.” (Dkt. 127 at 3). Because the defendant has made clear that he intends to argue that he had no ability to exercise control over any aspect of the Tornado Cash service, his suggestion that expert testimony about this very topic is irrelevant should be swiftly rejected.

The defendant also argues that evidence regarding his ability to control features of the Tornado Cash service should not be admitted because it cannot prove his intent to commit the charged crimes. (Dkt. 158 at 18). That is wrong on two counts. First, even if Werlau’s testimony were only relevant to show the defendant’s conduct, that is still a sufficient basis to admit the testimony regardless of whether it also goes to intent. Second, evidence about how the defendant actually conducted himself in operating the Tornado Cash service, including the control he exercised over certain features and the nature of the changes he made to it over time, is directly relevant to his state of mind. *See, e.g., United States v. Whitehead*, 579 F. App’x 46, 47 (2d Cir. 2014) (a “jury may infer guilty intent from pattern of conduct”). Moreover, the defendant’s *failure* to make certain changes to the service, even when he knew that the service was conducting money laundering transactions, and even though those changes were feasible for him to make, as

established by expert testimony and otherwise, is also relevant evidence of his intent to continue to participate in those unlawful transactions. Indeed, as a factual matter, there will be evidence that the defendant on several occasions rejected suggestions regarding implementing KYC on the Tornado Cash service, evidencing both the ability to make that change and the defendant's state of mind in refusing to do so. *See United States v. Dupree*, No. 10 Cr. 627, 2012 WL 5333946, at *24 (E.D.N.Y. Oct. 26, 2012), *aff'd*, 620 F. App'x 49 (2d Cir. 2015) (noting that a jury could infer from a defendant's "failure to disclose" a fraud that the defendant "knew that his conduct was unlawful and that he possessed the intent to continue" the criminal conduct).

The defendant's final point—that Werlau should not be permitted to testify about "lay matters which a jury is capable of understanding and deciding without the expert's help" (Dkt. 158 at 19 (quotation marks and citation omitted))—has no bearing on the testimony at issue here. A lay jury is not capable of examining the source code and understanding how it works, the significance of particular code upgrades that were made over time, and how the code could have been revised or updated further. That is the expert testimony that Werlau will provide to assist the jury in evaluating the evidence in this case.

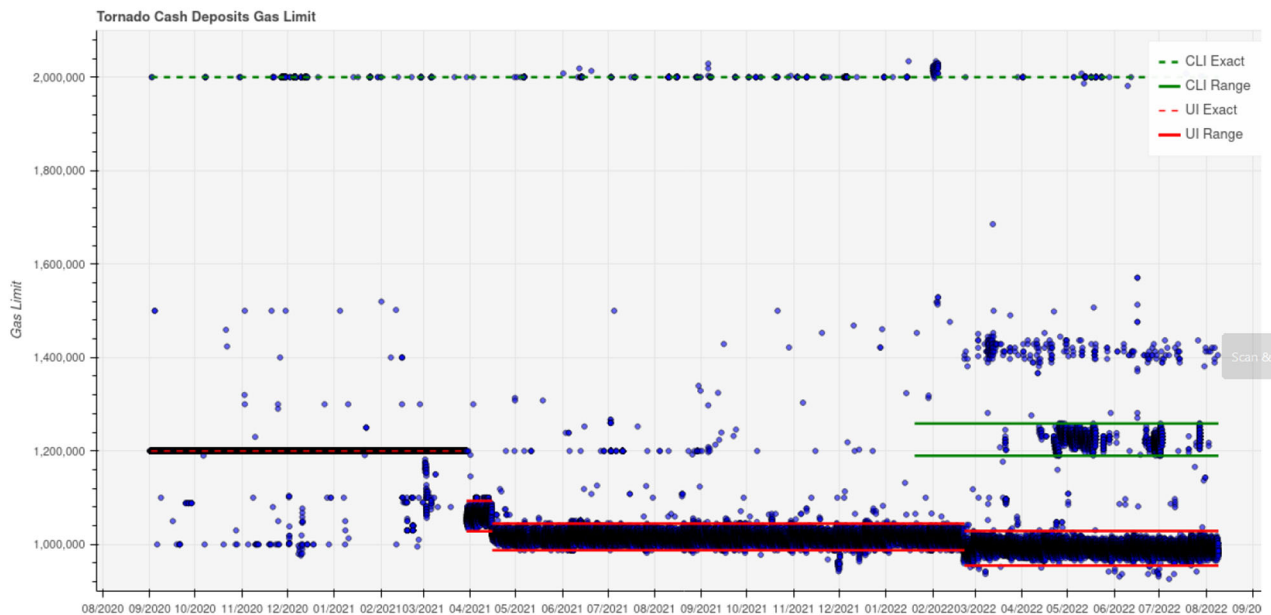
E. Werlau's Testimony Regarding the "Gas Ratio" Is Admissible

1. Background

The defendant's final argument regarding Werlau's testimony relates to Werlau's analysis of the "gas limit" and "gas ratio" for Tornado Cash deposits, and how this information can be used to determine whether deposits were made using the UI or the CLI. Because the defendant's motion does not accurately describe this analysis, the Government provides the following summary of the disclosed testimony.

As Werlau explains, the Ethereum network charges what is referred to as a "gas fee" to cover the cost of validating each transaction. (Werlau Disclosure ¶ 4). Thus, when a transaction is

initiated on the blockchain, the instructions for the transaction also communicate “the amount of gas that it is willing to use to complete the transaction, which is commonly referred to as the ‘gas limit.’” (*Id.* ¶ 22). In the case of the Tornado Cash service, the UI and CLI were set up to decide the gas limit for each deposit they executed, and include that as part of the transaction instructions. Then, when the transaction is completed, the blockchain records both the gas limit that was initially set, and the amount of gas that was actually used, and the relationship between these two numbers is referred to as a “gas ratio.” Thus, when large numbers of transactions have similar gas limits or gas ratios, this can be used to determine that they likely originated using the same method. (*Id.*). To apply this method to the Tornado Cash service, Werlau reviewed blockchain data for all Tornado Cash deposits from the charged time period, a total of approximately 140,000 deposits. Every deposit from this time period is represented by a dot in the chart below, which was one of the supporting materials produced with the Werlau disclosure (Dkt. 158-4 at 3):



Each dot represents a deposit, and the placement of the dot represents when it happened (on the x-axis) and the gas limit that it used (on the y-axis). From September 2020 until March 29,

2021, the UI had a hard-coded fixed gas limit of 1.2 million, and the chart shows that almost all transactions used that gas limit during the initial period. There are so many thousands of dots at exactly that gas limit that it appears to be a solid line until the UI was changed. Meanwhile, the CLI was initially hard-coded with a gas limit of 2 million, and a number of transactions (although not nearly as many) can be seen on the chart with that limit.

Based on the source code, Werlau identified that the UI was revised on March 29, 2021; instead of a hard-code limit, the UI would estimate the gas limit for each transaction. As can be seen on the chart, the gas limit for the overwhelming majority of deposits immediately changed on that date. Whereas previously almost all transactions were exactly at a gas limit of 1.2 million, after March 29, 2021, almost all transactions are concentrated in a narrow range around a lower gas limit. Based on the source code, Werlau also identified that there were changes to the UI's gas limit method on April 15, 2021, and on February 21, 2022, and those dates also show an immediate change in the distribution of transaction data to different ranges.

Because the data is so voluminous and because there were such immediate and obvious changes in the gas-limit data each time the UI was changed, this comparison of the dates of code changes to the blockchain data is already a sufficient basis to evaluate Werlau's opinion that the concentrated bands of transactions represent UI transactions. But to check and verify the methodology, Werlau relied on three additional steps. First, "thousands of deposits were simulated" using "code matching the relevant gas estimation code from the UI" for each time period. (Dkt. 158-4 at 5).³ The simulated transactions allowed Werlau to identify a range of gas

³ The defendant's motion notes that the code that was used to conduct this simulation was not produced. (Dkt. 158 at 22). Upon reviewing the defendant's motion, the Government reviewed its files and realized that the code used for the simulations had been blocked by its internal spam filters, which block "executable computer code," and was therefore inadvertently not included with the disclosure. Upon discovering this issue, the Government promptly produced the code.

limits that the UI would generate for deposits during each time period, which is represented by the red lines on the chart above. This simulation provides additional verification that the concentrated bands of deposits were in fact UI transactions, because the simulated range of UI gas limits aligns with the actual range observed in historical transaction data. Second, in addition to calculating an overall range, the actual gas limits for particular historical transactions were compared to the simulated gas values for simulated transactions, revealing a high percentage of “near or exact match[es]” between the two. (Dkt. 158-4 at 10-11). This high percentage of matches provides further verification that the methodology used to estimate UI transactions was reliable. Third, Werlau was provided with the blockchain data for certain blockchain deposits that are known to the Government to have been made using the UI, because the person who made those deposits has told the Government he used the UI.⁴ Werlau’s methodology correctly identified these deposits as having been made using the UI. (Werlau Rebuttal Disclosure ¶ 3).

Werlau also performed a similar analysis for the CLI, which originally had a hard-coded gas limit of 2 million, and then was updated by the defendant on January 20, 2022, which is represented by the green lines on the chart. (Dkt. 158-4 at 9). Werlau’s conclusion is that 96.16% of all Tornado Cash deposits used the UI, and 2.78% used the CLI. (Dkt. 158-4 at 10).

2. Werlau’s Gas Limit Analysis is Admissible

The defendant levels various scattershot arguments against Werlau’s opinion regarding the use of the gas limit and gas ratio to attribute transactions to the UI and CLI. None warrants preclusion of this testimony, as the arguments generally mischaracterize the testimony and at most

⁴ The defense argues that the identity of this person is not disclosed in the Werlau disclosure. (Dkt. 158 at 21). This person will be a trial witness, and the Government will produce his 3500 material at the same time as other 3500 material in the case. The defense will be free to cross him on how he accessed the UI, at what time(s), and how often.

go to weight rather than admissibility. In determining the admissibility of expert testimony, the Second Circuit has explained that “Rule 702 embodies a liberal standard of admissibility for expert opinions.” *United States v. Napout*, 963 F.3d 163, 187 (2d Cir. 2020) (quoting *Nimely v. City of New York*, 414 F.3d 381, 395 (2d Cir. 2005)). The Court serves its “gatekeeping role by ensuring that an expert’s testimony both rests on a reliable foundation and is relevant to the task at hand.” *Id.* at 187-88 (quoting *Daubert v. Merrell Dow Pharms.*, 509 U.S. 579, 597 (1993)). Here, the relevance of whether transactions used the UI or CLI is uncontested. And as explained above, Werlau’s testimony is based on a reliable foundation—it combines analysis of the source code for the UI and CLI with blockchain data for 140,000 transactions, and is cross-checked against thousands of simulated transactions to verify that the ranges used to attribute transactions correspond to actual gas limits that were generated by deposits using the UI or CLI. The defendant’s arguments do not come close to showing that this methodology is “speculative or conjectural or based on assumptions that are so unrealistic and contradictory as to suggest bad faith or to be in essence an apples and oranges comparison,” which is the standard for preclusion. *Id.* at 188. Rather, the defendant raises “other contentions that [an expert’s] assumptions are unfounded,” which “go to the weight, not the admissibility, of the testimony.” *Id.*

First, the defendant argues that the methodology has been insufficiently “tested,” claiming that the only testing is Werlau’s comparison to the small number of transactions for which the Government has witness testimony regarding use of the UI. (Dkt. 158 at 21). But as detailed above, the defendant completely ignores the fact that Werlau in fact performed extensive additional testing to verify his attribution methodology, by simulating thousands of transactions and using that simulation both to generate a range of potential gas limits generated by the UI and to compare particular simulated transactions to historical transactions. The fact that these simulated

transactions produced a range that matches so precisely with the actual historical data is a striking verification of the methodology.⁵

The defendant also argues that Werlau’s methodology has not been subject to peer review, that Werlau does not disclose an error rate, and that it has not been accepted in the relevant community. (Dkt. 158 at 22-23). But while each of these are factors that the Court “*may consider*” in evaluating the reliability of Werlau’s testimony, the Second Circuit and the Supreme Court have made clear that “the test of reliability is ‘flexible,’ and *Daubert*’s list of specific factors neither necessarily nor exclusively applies to all experts or in every case. Rather, the law grants a district court the same broad latitude when it decides *how* to determine reliability as it enjoys in respect to its ultimate reliability determination.” *Restivo v. Hessemann*, 846 F.3d 547, 576 (2d Cir. 2017) (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152 (1999) (quotation marks and citations omitted; emphasis in original)). Here, the detailed explanation of Werlau’s methodology, the voluminous historical data underlying it, and the multiple verification steps he took, all counsel in favor of finding the testimony sufficiently reliable to be admitted. The defendant’s critiques of the methodology do not rise to the level of showing that it is “speculative or conjectural.” *Napout*, 963 F.3d at 188.

⁵ The defendant also contends that Werlau did not apply the methodology “consistently,” pointing to a technical discrepancy between the initial disclosure and the rebuttal disclosure that affected a small number of transactions but not enough to change the overall percentage. (Dkt. 158 at 21; *see* Werlau Rebuttal Disclosure ¶ 3 (noting “slight revisions” from initial disclosure)). That argument is a red herring, as Werlau’s testimony will rely on the methodology as set forth in the rebuttal disclosure and the results that it generated, and the defendant does not even attempt to suggest that there is any inconsistency in this methodology. To the extent the defendant seeks to explore the slight difference between the initial disclosure and the subsequent disclosure, the appropriate place to do that is in cross-examination. *Henkel v. Wagner*, 2016 WL 1271062, at *11 (S.D.N.Y. Mar. 29, 2016) (“To the extent Defendants wish to question the reliability” of materials on which an expert relied, or “highlight documents that [the expert] may have failed to consider, cross-examination is an appropriate way of attacking weak expert testimony, rather than complete exclusion.”).

For instance, the defendant highlights the possibility, which Werlau acknowledges, that an individual Tornado Cash user who was not using the UI might have happened to set a gas limit that was similar to the limit used by the UI. (Dkt. 158 at 22). That possibility, however, does not call into question the overall reliability of Werlau’s methodology, especially given that the range of gas limits for the vast majority of deposits (more than 95%) shifted immediately whenever the UI’s method for calculating a gas limit was modified. More importantly, this is exactly the sort of quibbling about details that goes to the weight, rather than the admissibility, of the testimony. “As long as there is a factual basis for an expert’s decision, the inclusion or exclusion of certain data points, when making an estimate, generally falls within the range where experts might reasonably differ, making the duty of determining the weight and sufficiency of the evidence on which the expert relied one for the jury, rather than the trial court.” *PRCM Advisers LLC v. Two Harbors Inv. Corp.*, No. 20 Civ. 5649 (LAK) (BCM), 2025 WL 1276513, at *17 (S.D.N.Y. May 2, 2025); *see also Capri Sun GmbH v. Am. Beverage Corp.*, 595 F. Supp. 3d 83, 135 (S.D.N.Y. 2022) (declining to exclude expert opinion “for relying on unverified revenue figures as part of his analysis, for cherry-picking among sales data, and for underlying limited verification of data,” because “the asserted divots in [the expert’s] data and approach are best left for adversarial testing at trial”); *DoubleLine Cap. LP v. Odebrecht Fin., Ltd.*, 2024 WL 1115944, at *11 (S.D.N.Y. Mar. 14, 2024) (when constructing a study, researchers “necessarily rely on their discretion, to some degree,” to determine what information or data “meets their selection criteria”).

The defendant’s final argument regarding the gas limit analysis is that some of the underlying documentation that the Government provided as part of its disclosure was prepared by a person other than Werlau. (Dkt. 158 at 23). That argument borders on the frivolous. In both his initial and rebuttal disclosures, Werlau provides a detailed explanation of the methodology he used

to form his opinions, with reference to the substantial supporting documentation that was produced in connection with the disclosures. (Werlau Disclosure ¶ 22; Werlau Rebuttal Disclosure ¶ 3). To assist the defense in analyzing Werlau’s opinions, the Government produced a number of more granular explanations of the step-by-step process behind the disclosed opinions, including in documents that were authored by analysts who assisted Werlau. There is nothing remotely unusual or improper about an expert witness being assisted by others in collecting and compiling information that the expert uses to form his opinion. The rules expressly contemplate that an expert may base his opinion on “facts or data in the case that the expert has been made aware of or personally observed.” Fed. R. Evid. 703. In applying this rule to a software-code expert, another court in this District recently explained that the expert was “not required to personally examine [the software] in order to offer an admissible opinion. He instead permissibly relies on documents and testimony provided to him by counsel, particularly as it relates to the purpose, scope and operation of [the software].” *PRCM Advisors LLC v. Two Harbors Inv. Corp.*, No. 20 Civ. 5649 (LAK) (BCM), 2025 WL 1276513, at *10 (S.D.N.Y. May 2, 2025); *see also, e.g., Gussack Realty Co. v. Xerox Corp.*, 224 F.3d 85, 95 (2d Cir. 2000) (“The expert need not have conducted his own tests.”). Here, as he will explain, Werlau did in fact personally review the code and the blockchain data in forming his opinion, and he applied the methodology as disclosed. But even if Werlau had based his opinion on work performed by others, the rules are clear that this is permissible as long as an expert “in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject.” Fed. R. Evid. 703.

II. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Stephan George

The Government intends to call IRS-CI Special Agent Stephan George to present his tracing analysis showing that the defendant engaged in a complex set of transactions converting

TORN tokens and cryptocurrency withdrawn from the Tornado Cash service into fiat currency or other types of cryptocurrency. (Dkt. 158-6 (“George Disclosure”) at ¶¶ 4-7; Dkt. 157 at 30-31). George will describe how the funds traced to those transactions were used, in part, to purchase assets, including two houses. (*Id.*). In addition, George will present tracing analysis showing that, in August 2022, the Defendant used a cryptocurrency account held in the name of another person to liquidate TORN and convert it to other cryptocurrency worth about \$12 million. (George Disclosure ¶ 9).

The defendant does not challenge George’s qualifications or the basis for the expert opinions he proposes to testify to, but instead argues that this evidence is “irrelevant and prejudicial.” The defendant presumes that the purpose of offering the testimony is to prove forfeiture, and from there argues that it is improper to introduce forfeiture at trial and that the TORN traced does not represent criminal proceeds. That completely misses the mark. As explained in the Government’s motions *in limine* and in opposition to the defendant’s motions *in limine*, evidence of the defendant’s financial transactions involving TORN and the Tornado Cash service, including but not limited to sales in June and August of 2022, are relevant to proving the criminal offenses in the Indictment. (Dkt. 157 at 30-32; Dkt. 173 at 23-27). To summarize, the defendant and his co-conspirators created TORN and distributed it to themselves through a variety of means, including through vouchers distributed and redeemed through smart contracts. (George Disclosure ¶ 2). This and other evidence, including evidence showing the defendant’s own use of the service, will demonstrate the defendant’s control over the service, how introducing more liquidity into the service increased the total size of the mixed deposits and facilitated concealment of illicit proceeds, and the defendant’s profit motive for continuing to participate in the

conspiracies to launder money, transfer criminal proceeds, and violate sanctions. This evidence directly supports all three charges in the Indictment. (*See* Dkt. 157 at 31-32; Dkt. 173 at 23-27).

Evidence that the defendant concealed his and his co-conspirators' gains from the operation of the Tornado Cash service, such as tracing showing the complex network of transactions he utilized and the timing of those transactions, combine with other circumstantial evidence to show direct evidence of the charged conspiracies and the defendant's consciousness of guilt. For example, on August 8, 2022, shortly after the defendant was informed that the Office of Foreign Assets Control (OFAC) had sanctioned Tornado Cash, he almost immediately initiated transactions to liquidate TORN for himself and his co-conspirators. The defendant steadily liquidated TORN over at least the next whole day, which he converted into the cryptocurrency he distributed to himself and his co-conspirators.⁶ This evidence is admissible in the Government's case-in-chief even if it is also relevant in a subsequent forfeiture proceeding. *See* Fed. R. Crim. P. 32.2(b)(1)(2) (the factfinder's determination of what specific property is subject to forfeiture "may be based on evidence already in the record ... and on any additional evidence or information submitted by the parties and accepted by the courts as relevant and reliable.").⁷

⁶ Because the probative value of this evidence is to show, in part, the defendant's real time reaction to the sanctions against Tornado Cash, it is of no moment that the sanctions were later rescinded. *See generally* Dkt. 120 at 6-14 (the decision in *Van Loon* is consistent with the charged offenses and does not negatively affect them). *Cf.* Dkt. 157 at 35-36 (evidence of defendant's effort to preserve Tornado Cash service operations is admissible); *Id.* at 59-60 (the Court should preclude defendant from introducing evidence regarding the legality of OFAC's sanctions on the Tornado Cash service). The Government further addresses this issue in its opposition to the defendant's motions *in limine*. (Dkt. 173 at 29-36).

⁷ The defendant is correct that the issue of whether the defendant purchased assets with crime proceeds or funds involved in or traceable to money laundering is a question of nexus for a forfeiture proceeding. But at trial, the transactions and tracing of TORN to the defendant's purchase of assets is being offered as evidence of the crimes charged for the reasons stated herein and in other briefing.

III. The Court Should Deny the Defendant’s Motion to Preclude the Testimony of Joel DeCapua

The Government intends to call FBI Special Agent Joel DeCapua as an expert to testify regarding his analysis and tracing of cryptocurrency transactions, and in particular regarding his tracing of the proceeds of certain criminal incidents to the Tornado Cash service. (Dkt. 158-10 (“DeCapua Disclosure”) at 1). In addition to some background testimony to explain how blockchain data can be used to trace cryptocurrency transactions (*id.* at ¶¶ 1-2), DeCapua will testify regarding his tracing of the proceeds from 31 criminal incidents dating from September 2020 to July 2022, which were deposited into the Tornado Cash service. (*Id.* ¶¶ 3-4). He identified a total amount of approximately \$1.191 billion in criminal proceeds that were deposited into the Tornado Cash service. (*Id.* ¶ 5). For some of these incidents, DeCapua also used blockchain data to identify the gas limit and gas ratio for the deposits of criminal proceeds that were made into the Tornado Cash service. (*Id.* ¶ 6). Separate from his analysis of these criminal incidents, DeCapua also used blockchain data to identify the total volume of cryptocurrency deposited to and withdrawn from the Tornado Cash ETH pools, including the inflows and outflows and the aggregate balance of the pools over time, and will provide testimony regarding these volumes around the times of some of the criminal incidents. (*Id.* ¶ 7). Finally, DeCapua traced the flow of funds from a particular Ethereum address—the address referred to in the Indictment as the “0x098B716 Address,” which was designated as sanctioned on April 14, 2022—into the Tornado Cash service. (*Id.* ¶ 8).

The defendant’s motion claims to challenge the entirety of DeCapua’s testimony, but the only issue the defendant raises with this testimony is the purported reliance on hearsay to identify the sources of the funds that DeCapua traced in paragraphs 3 through 6 as being criminal incidents. The defendant does not challenge DeCapua’s expertise in tracing cryptocurrency transactions or

the methodology DeCapua used to trace the transactions. Nor does the defendant raise any challenge to the other parts of DeCapua's testimony. In particular, paragraphs 7 and 8 of the DeCapua disclosure are based solely on blockchain data as opposed to any other information regarding any criminal exploits.

With respect to the identification of criminal exploits that informs DeCapua's testimony in paragraphs 3 through 6, the defendant argues that this testimony is inconsistent with case law regarding the limits of law enforcement witness testimony, and in particular that it impermissibly relies on hearsay and violates the Confrontation Clause. Those arguments, however, rely on inapposite case law about the so-called "officer expert," a law enforcement officer who testifies about the structure, jargon, and internal workings of a criminal organization based on his experience investigating that organization. DeCapua's testimony bears no resemblance to that type of testimony and does not raise any of the concerns recognized by courts in addressing that type of testimony, including the hearsay and Confrontation Clause issues argued by the defendant. On the contrary, DeCapua's testimony is a traditional and accepted form of expert testimony, and to the extent that it relies on hearsay, it does so in a manner consistent with the express language of the Federal Rules of Evidence and the case law.

A. Expert Testimony Based in Part on Hearsay Is Admissible, and the "Officer Expert" Cases on Which the Defendant Relies Are Inapposite

In his motion, the defendant relies on a line of cases addressing what the Second Circuit has referred to as the "officer expert," a law enforcement witness who uses his or her "experience and training to speak to the operation, symbols, jargon, and internal structure of criminal organizations." *United States v. Mejia*, 545 F.3d 179, 190 (2d Cir. 2008). While the Second Circuit has "repeatedly upheld the admission" of such testimony, *id.* at 190, it has also recognized that such officers could overstep the bounds of their expertise if they "testify about the meaning of

conversations in general, beyond the interpretation of code words,” or if they simply recycle information learned from “hearsay and custodial interrogations,” rather than relying on their general expertise about the subject matter, *id.* at 192-93. Thus, for example, in *United States v. Dukajgini*, a DEA agent repeatedly interpreted recorded conversations on the basis of his “knowledge of the investigation” and “also from speaking with *cooperating individuals* and *from speaking with cooperating defendants*.” 326 F.3d 45, 59 (2d Cir. 2003) (emphasis in original). Because this testimony did not involve the agent “translating drug jargon, applying expert methodology, or relying on his general experience in law enforcement,” the Second Circuit held that it crossed the “line between permissible and impermissible reliance on hearsay.” *Id.*

The testimony at issue here bears no resemblance to the “officer expert” testimony at issue in *Mejia*, *Dukajgini*, and similar cases. DeCapua is not a case agent in this case, he did not interview any individuals or rely on any law enforcement investigative materials, and he is not being offered as an expert in the structure or jargon of criminal organizations. Rather, DeCapua is an expert in “cryptocurrency tracing and blockchain analysis” who has years of experience in analyzing “the laundering of proceeds from network intrusions and ransomware incidents through the use of cryptocurrency.” (DeCapua Disclosure at 1). He applied that general expertise in this case. While DeCapua did rely on public reports and statements from victims to assist him in identifying criminal exploits, he is not simply recycling those statements, as was the case in *Dukajgini*. As explained in DeCapua’s disclosure, he “identified wallet addresses tied to the incident and reviewed information about those wallet addresses available on a public blockchain explorer, such as Etherscan, to identify whether there was activity that corresponded to the public descriptions of the incident.” (*Id.* ¶ 4). Based on his extensive experience in investigating such incidents, he explains that the method he employed in this case “is a commonly employed method

for tracing the proceeds of criminal incidents used by cryptocurrency investigators.” (*Id.*). Notably, the defendant does not question that description or the fact that this is a commonly employed method used by experts in this area. Thus, DeCapua’s testimony falls within the long-recognized rule that “expert witnesses can testify to opinions based on hearsay or other inadmissible evidence if experts in the field reasonably rely on such evidence in forming their opinions.” *United States v. Locascio*, 6 F.3d 924, 938 (2d Cir. 1993); *see also* Fed. R. Evid. 703.

Indeed, in a variety of contexts, courts have regularly permitted expert witnesses to rely on hearsay in forming their opinions, provided that the expert’s opinion involves the application of expertise and not merely the repetition of the hearsay. *See, e.g., United States v. Torres*, No. 20 Cr. 608 (DLC), 2021 WL 1947503, at *7 (S.D.N.Y. May 13, 2021) (permitting Government to introduce expert testimony where the expert’s “research methodology may be based on qualitative interviews that involve listening to the statements of domestic abuse victims, but her testimony will involve the synthesis and interpretation of those statements, rather than the mere conveyance of those statements to the jury”); *United States v. Diakhoumpa*, 171 F. Supp. 3d 148, 150 (S.D.N.Y. 2016) (permitting Government to call as expert witnesses “import specialists with Customs and Border Protection (‘CBP’) who examined the counterfeit items and made the determination that the items lack authenticity” and whose testimony was based in part on “information provided by trademark holders to CBP for purposes of training its import specialists”); *United States v. Prevezon Holdings, Ltd.*, 251 F. Supp. 3d 684, 697 (S.D.N.Y. 2017) (permitting Government to present financial tracing analysis in which “many of the transactions were identified as money laundering transactions based on their structure and characteristics—e.g., time at which they were opened, timing and similar patterns of transactions, fictitious business purposes, shell accountholders”).

This type of testimony is in stark contrast to the testimony at issue in *Mejia*, the primary case on which the defendant relies. In *Mejia*, the Second Circuit found that an expert was not relying on general expertise when he simply repeated “the results of the Task Force investigation” drawn from various hearsay sources, such as the number of firearms recovered from MS-13 gang members or the number of murders committed by those gang members. 545 F.3d at 194-95. By contrast, here, DeCapua’s testimony rests on the combination of his gathering publicly available information and then verifying that through detailed analysis of blockchain transactions to identify activity that, in his experience, is consistent with criminal exploits—a critical step wholly ignored by the defendant in his argument. For instance, the Government produced voluminous notes and transaction records for the DeCapua disclosure that document various aspects of these transactions that informed DeCapua’s conclusion, such as the presence of sudden large outflows of multiple types of tokens from exchange wallets to single wallets, the rapid conversion of those tokens to ETH, and the cycling of the proceeds through multiple intermediary wallets prior to their deposit into the Tornado Cash service. As such, unlike any of the cases defendant cites, DeCapua is not “simply repeating hearsay evidence without applying any expertise whatsoever.” (Dkt. No. 158 at 39 (quoting *Mejia*, 545 F.3d at 197)).

Indeed, in a similar recent case, a district court admitted cryptocurrency tracing evidence that rested on hearsay to a greater degree than anything at issue here. In *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024), the Government introduced expert testimony regarding tracing of cryptocurrency to particular darknet marketplaces based on a tool developed by the company Chainalysis. The Chainalysis tool based its attributions in part on “data and information obtained off-chain from, among other things, Chainalysis’s clients and partners (which include global cryptocurrency exchanges), government subpoenas, and data leaks.” *Id.* at 83. As the district court

recognized, “a jury is well equipped to decide, through cross examination,” whether it was reasonable for an expert to rely in part on this hearsay information in forming opinions about the source of particular cryptocurrency transactions. *Id.* Here, the jury is even more well-equipped to decide, because DeCapua’s testimony does not depend on a proprietary algorithm that incorporates hearsay, but instead on his own expert analysis of blockchain data in conjunction with public reporting to form the type of conclusions that he reaches regularly in his work as a cryptocurrency tracing analyst who responds to criminal incidents. Thus, the evidence should be admitted.

B. DeCapua’s Proposed Testimony Does Not Convey Hearsay or Violate the Confrontation Clause

Many of the arguments in the defendant’s motion are in part based on misreading the nature of DeCapua’s disclosure, the materials on which he relied, and the expert opinions he will offer. In particular, the defendant’s motion overlooks that DeCapua’s identification of criminal exploits rests in large part on evidence that is admissible and that the Government intends to admit at trial. For example, the defendant notes that the DeCapua disclosure references “documentation of the incidents that was sent by the victims or law enforcement,” and then suggests that this means DeCapua will be testifying about statements made by victims to law enforcement. (Dkt. 158 at 41). Perhaps the defense should have read the rest of that sentence in DeCapua’s disclosure, which explains that DeCapua “reviewed documentation of the incidents that was sent by the victims or by law enforcement *to the Tornado Cash founders.*” (Dkt. 158-10 ¶ 4 (emphasis in original)). The documents referenced here are documents from the discovery in this case that were also included as part of DeCapua’s disclosure. These documents are direct evidence of the defendant’s knowledge that particular transactions involved the proceeds of criminal activity, and the Government intends to introduce these documents as trial exhibits to prove the defendant’s knowledge.

To take one example of a victim statement to the defendant, in October 2020, an employee of a victimized cryptocurrency exchange (“Cryptocurrency Exchange-1”) sent the defendant and his co-founders an email telling them that “the hacker of [Cryptocurrency Exchange-1] has transferred the ETH to your platform,” and providing them with a link to the blockchain data documenting this. (Ex. A). Similarly, DeCapua relied on information that law enforcement officers sent *to the defendant* about criminal exploits during the time period of the charged conspiracies. For example, after a cryptocurrency platform was compromised in 2021, a law enforcement officer contacted the defendant and his co-founders, telling them that “the hacker used your service to swap tokens” and providing the defendant with links to blockchain data regarding the incident—the very same blockchain data on which DeCapua relied in conducting his analysis. (Ex. B).

The defendant does not argue, nor could he, that DeCapua should be precluded from testifying about tracing of proceeds from incidents that the defendant himself was made aware of at the time, or that relying on admissible evidence about such incidents would raise hearsay or Confrontation Clause issues. Instead, he attacks a straw man by suggesting that DeCapua relied on victim statements made to law enforcement. That is incorrect, DeCapua did not rely on any such statements in forming his opinions. The defendant’s citations to cases casting doubt on law enforcement testimony that relies on such statements are therefore inapposite.

To be sure, DeCapua also relied on public statements made by victims regarding criminal exploits, and the Government provided the defense with a detailed disclosure of those statements to assist the defense in reconstructing and analyzing DeCapua’s tracing work. (Dkt. 158-11). And the Government does not expect that there will be evidence admitted at trial regarding all of the criminal incidents that are the subject of DeCapua’s overall tracing. For some incidents, DeCapua’s identification of them as criminal exploits is based only on the combination of the

public reporting and his independent blockchain analysis, and does not draw on anticipated trial testimony or exhibits.

As discussed above, because experts in the field do in fact rely on such public information in forming their opinions, and because DeCapua applied his expertise and training in forming his opinions, his testimony regarding all the cryptocurrency incidents is admissible, even those for which there will not be separate evidence introduced at trial. However, even if the Court agreed with the defendant that DeCapua should not be permitted to testify about any criminal incidents aside from those that will be the subject of other trial evidence (and it should not), his testimony should still be admitted regarding the tracing of the proceeds of any criminal exploits that are the subject of trial evidence. As detailed in its opposition to the defendant's motions *in limine*, the Government intends to introduce victim testimony to demonstrate that certain criminal incidents occurred and evidence from the defendant's own emails and chats to demonstrate that the defendant was made aware of certain criminal incidents. These incidents are the source for the majority of the criminal proceeds identified in the DeCapua disclosure, amounting to over \$950 million out of the \$1.191 billion in criminal proceeds that DeCapua traced. Thus, even if everything in the defendant's motion were correct, DeCapua's testimony as to these criminal incidents should still be admitted.

IV. The Court Should Deny the Defendant's Motion to Preclude the Testimony of John Pisa-Relli

The defendant's motion to preclude the testimony of OFAC employee John Pisa-Relli is meritless. As set forth in the Government's response to the defendant's motions *in limine*, testimony from an OFAC witness is necessary to establish elements of the crime charged in Count Three: that there were in fact sanctions on the Lazarus Group and on the particular wallet address that was designated as property of the Lazarus Group, and that the defendant and his business did

not have a license to transact with the Lazarus Group. These are facts, and the appropriate witness to establish these facts is a witness from OFAC. Thus, witnesses from OFAC regularly testify to similar facts in similar cases and are not designated as expert witnesses. *In re 650 Fifth Ave. & Related Properties*, No. 08 Civ. 10934 (KBF), 2017 WL 6419014, at *1 (S.D.N.Y. May 30, 2017) (denying defense motion to compel expert report in connection with testimony of OFAC witness, similar to the OFAC testimony expected in this case, “regarding areas about which [the witness] has first-hand knowledge based on her expertise,” where she “is not going to offer opinions of any sort or legal conclusions”).

The defendant does not cite any authority suggesting that such testimony is expert testimony, much less that it is inadmissible expert testimony. Instead, he primarily relies on the Second Circuit’s decision in *Bank of China, New York Branch v. NBM LLC*, 359 F.3d 171, 181 (2d Cir. 2004). But that case involved a bank employee who was asked to opine on what constituted “typical” banking transactions, among other matters. The Second Circuit held that such testimony was opinion testimony that required qualification as an expert. But the Government does not intend to elicit opinions from the OFAC witness, who will instead testify about the fact that certain sanctions were announced by OFAC at particular times, and that OFAC records indicate that the defendant did not obtain a license. The defendant’s attempt to challenge this testimony should be rejected.

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should deny the defendant's motions to preclude the Government's expert witnesses.

Respectfully submitted,

JAY CLAYTON
United States Attorney for the
Southern District of New York

By: /s/ Thane Rehn
Ben Arad
Benjamin A. Gianforti
Thane Rehn
Assistant United States Attorneys

Kevin Mosley
Special Assistant United States Attorney
(212) 637-2354

Dated: June 18, 2025
New York, New York